arXiv:0804.1538v1 [quant-ph] 9 Apr 2008

More Efficient Purifying scheme via Controlled- Controlled NOT Gate

N. Metwally [1]and A.-S. Obada [2]

[1] *Math. Dept., Faculty of Science, South Valley University, Aswan, Egypt.*

[2] *Math. Dept., Faculty of Science, Al-Azhar University, Cairo, Egypt.*

Abstract

A new modified version of the Oxford purification protocol is proposed. This version is based on the controlled-controlled NOT gate instead of controlled NOT in the original one. Comparisons between the results of the new version and the original and an earlier modification are given. It is found that the new version converges faster and consumes fewer initial qubit pairs of low fidelity per final qubit pair of high fidelity.

1 Introduction

It is well known that to perform most of the quantum information schemes efficiently, one requires maximally entangled states to be performed. However in reality, it is mandatory to consider the effect of the decoherence. In this situation, the maximally entangled states turn into partially entangled or product states. Therefore, these schemes my not be realized faithfully. Thus purifying these states is of a great importance in the context of quantum information. The entanglement purification, that is often required, distills a small number of strongly entangled pairs of qubits from a large number of weakly entangled pairs. This can be achieved by using local quantum operations, classical communication and measurements. Bennett et. al have proposed the first entanglement purification scheme which is called the IBM protocol [**?**]. This protocol assumes that the initial states are of Werner type state. The initial density state for the IBM protocol is given by: $\rho = x|\psi^-\rangle\langle\psi^-| + \frac{1-x}{4}I$ which means that an x fraction of the singlet state $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ [**?**] and the rest is randomized . Another standard protocol has been proposed by Deutsch

[1] e. mail:Nasser_ Metwally@hotmail.com

et al. and it is called the Oxford protocol [?]. This protocol is designed for quantum cryptography. The initial density operator for this protocol takes the form: $\rho_{Ox} = A|\phi^+\rangle\langle\phi^+| + B|\psi^-\rangle\langle\psi^-| + C|\psi^+\rangle\langle\psi^+| + D|\phi^-\rangle\langle\phi^-|$ where $|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ are the Bell basis. Since then many theoretical [?] and experimental[?] schemes have been proposed.

The standard protocols [?,?] are based on the controlled NOT operations, CN and Bell state measurements. The IBM protocol has been improved by Feng et al [?], where they considered the controlled-controlled NOT operation (CCN) instead of CN. They showed that the new version is more efficient than the original one. Because in order to get a final state of certain fidelity from pairs of the same fidelity, the successful purification probability is larger and the amount of resources minimally consumed is less. Also the Oxford protocol has been improved by Metwally, where in his version the usual local unitary transformations are only performed when they are really helpful [?]. For some initial states this modification makes the new version converges faster, more efficient and needs fewer operations. For some other initial states the two versions are equivalent.

In this *contribution*, we study the Oxford protocol in the dynamical variables i.e., Pauli's operators, σ_i and τ_i, where $i = 0, x, y, z$ for the first and the second qubit respectively. In this current version we consider the CCN operation instead of the CN. We see that the modification makes the suggested version more efficient. In section 2,we describe briefly the Oxford protocol Ox_1 and its first modification Ox_2[?]. Also we achieve the CN operation using the dynamical variables. Section 3 is devoted to a study of the second modified version, Ox_3. A comparison of the three protocols is discussed in section 4. Finally we summarize our results in section 5.

2 The Oxford protocol, Ox_1 and the first modified version, Ox_2

Assume that Alice and Bob are given an ensemble of the so called generalized Werner states or self transposed states [?], or simply Bell-diagonal states [?]and they are asked to use the Oxford protocol to purify them. The users pick two pairs of the form

$$\rho^{(1)} = \frac{1}{4}(1 + c_x\sigma_x^{(1)}\tau_x^{(1)} - c_y\sigma_y^{(1)}\tau_y^{(1)} + c_z\sigma_z^{(1)}\tau_z^{(1)}) \tag{1}$$

where

$$1 \geq |c_x| \geq |c_y| \geq |c_z| \geq 0 \tag{2}$$

the order being a matter of convention. These coefficients $c_i, i = x, y, z$ are related to the coefficient of the original Oxford protocol by the following relations:

$$\begin{aligned}
c_x &= A - B + C - D \\
c_y &= A - B - C - D \\
c_z &= A + B - C - D
\end{aligned} \tag{3}$$

The initial fidelities of states (**??**) are given by:

$$F_1 = \mathrm{tr}\left\{\rho^{(1)}\rho^{(1)}_{\phi^+}\right\} = \frac{1}{4}(1 + c_x + c_y + c_z) \tag{4}$$

where

$$\rho^{(1)}_{\phi^=} = \frac{1}{4}(1 + \sigma^{(1)}_x\tau^{(1)}_x - \sigma^{(1)}_y\tau^{(1)}_y + \sigma^{(1)}_z\tau^{(1)}_z). \tag{5}$$

Assume that Alice and Bob want to purify their pairs by using the *first* modified Oxford protocol Ox_2. To achieve this aim, they perform the Bilateral CN operation, see table 1, on the pairs, followed by measuring the target qubit(second pair) in the computational basis. They measure the z components of the target spin $\sigma^{(2)}_z$ and $\tau^{(2)}_z$. They keep those first pairs for which they get the same results for the measurements and discard the others. After one step purification, they get

$$\rho_{Ox_2} = \frac{1}{4}\left[1 + \frac{c_x c'_x + c_y c'_y}{1 + c_z c'_z}\sigma_x\tau_x - \frac{c_x c'_y + c_y c'_x}{1 + c_z c'_z}\sigma_y\tau_y \frac{c_z + c'_z}{1 + c_z c'_z}\sigma_z\tau_z\right] \tag{6}$$

this is another new Bell state with fidelity,

$$F_{Ox_2} = \frac{1}{4P_1}\left[(1 + c_z)^2 + (c_x + c_y)^2\right] \tag{7}$$

	$I^{(2)}$	$\sigma^{(2)}_x$	$\sigma^{(2)}_y$	$\sigma^{(2)}_z$
$I^{(1)}$	1	$\sigma^{(1)}_x\sigma^{(2)}_x$	$\sigma^{(1)}_y\sigma^{(2)}_x$	$\sigma^{(1)}_z$
$\sigma^{(1)}_x$	$\sigma^{(2)}_x$	$\sigma^{(1)}_x$	$\sigma^{(1)}_y$	$\sigma^{(1)}_z\sigma^{(2)}_x$
$\sigma^{(1)}_y$	$\sigma^{(1)}_z\sigma^{(2)}_y$	$\sigma^{(1)}_y\sigma^{(2)}_z$	- $\sigma^{(1)}_x\sigma^{(2)}_z$	$\sigma^{(2)}_y$
$\sigma^{(1)}_z$	$\sigma^{(1)}_z\sigma^{(2)}_z$	$-\sigma^{(1)}_y\sigma^{(2)}_y$	$\sigma^{(1)}_x\sigma^{(2)}_y$	$\sigma^{(2)}_z$

Table 1
Bilateral CN operation between the two qubits which is defined by $\sigma^{(1)}_\mu$ and $\sigma^{(2)}_\mu$. The same table is applied to the two qubits $\tau^{(1)}_\mu$ and $\tau^{(2)}_\mu$.

where $P_1 = \frac{1}{2}(1 + c_z^2)$, is the probability that Alice and Bob obtain coinciding outcomes in the measurement of target pair[?]. Now Alice and Bob have a new ensemble described by (**??**). If this ensemble does not obey the ordering required by (**??**), then Alice and Bob use local rotations to bring the state into the wanted form. These are rotations by $\pi/2$ about the x, y or z axis, namely

$$U_{12j} = e^{i\pi(\sigma_j - \tau_j)} \quad \text{and} \quad j = x, y, z. \tag{8}$$

In fact it is only necessary to ensure that $|c_z|$ is smaller than $|c_x|$ and $|c_y|$; the relative size of $|c_x|$ and $|c_y|$ does not matter. In the standard protocol, Ox_1 [?], Alice and Bob perform the transformation (**??**) in $x-$ direction on all pairs. This operation changes the positions of c_y and c_z. After applying the Bilateral CN operation and measuring the target qubits, Alice and Bob get a new ensemble with fidelity

$$F_{Ox_1} = \frac{1}{4P_2}\left[(1 + c_y)^2 + (c_x + c_z)^2\right] \tag{9}$$

where $P_2 = \frac{1}{2}(1 + c_y^2)$ is the probability that Alice and Bob's measurements are the same.

3 The second modified protocol, Ox_3

Before performing this protocol, one needs to describe the controlled-controlled Not, CCN. It is a three qubit gate, two of them are used as a control qubit and the third is a target. Mathematically it takes the following form,

$$\begin{aligned} CCN = \frac{1}{4}\Big[&(1 + \sigma_z^{(1)})(1 + \sigma_z^{(2)})\sigma_x^{(3)} + (1 + \sigma_z^{(1)})(1 - \sigma_z^{(2)}) \\ &+ (1 - \sigma_z^{(1)})(1 + \sigma_z^{(2)}) + (1 - \sigma_z^{(1)})(1 - \sigma_z^{(2)})\Big] \end{aligned} \tag{10}$$

The target qubit pairs change only when the two control qubits are in the state 1. In a generic form one can write its effect as $CCN|abc\rangle = |ab, c \oplus a.b\rangle$. As an example it transforms the vector $|\phi_1^+\phi_2^+\phi_3^-\rangle$ to $\frac{1}{2}[|\phi_1^+\phi_2^+\phi_3^-\rangle + |\phi_1^-\phi_2^+\phi_3^-\rangle + |\phi_1^+\phi_2^-\phi_3^-\rangle - |\phi_1^-\phi_2^-\phi_3^-\rangle]$. It is possible to consider the effect on the dynamical variables, but its form is too complicated to be written in this text.

Assume that Alice and Bob are given an ensemble of identical pairs in the form of equation (**??**). To perform the second modified version of the Oxford protocol Ox_3, they pick three pairs and both of them perform the transformation (**??**) on all pairs. After applying the CCN operations , they measure the

target qubits in the projection $|\phi^+\rangle_{A_1A_2}\langle\phi^+|\otimes|\phi^+\rangle_{B_1B_2}\langle\phi^+|+|\phi^-\rangle_{A_1A_2}\langle\phi^-|\otimes|\phi^-\rangle_{B_1B_2}\langle\phi^-|$, where A_1A_2 and B_1B_2 stands for the first and the second qubits for Alice and Bob respectively. They will keep those pairs for which the measurement results coincide. These pairs are used for the second round. After one step purification they get a new ensemble of states,

$$\rho_{Ox_3}=\frac{1}{4}(1+c_x^{new}\sigma_x\tau_x+c_y^{new}\sigma_y\tau_y+c_z^{new}\sigma_z\tau_z) \tag{11}$$

with a fidelity

$$F_{Ox_3}=\frac{1}{2P_3}\left[(A^2+D^2)A+(B^2+C^2)C\right] \tag{12}$$

and,

$$\begin{aligned}C_x^{new}&=A_{new}-B_{new}+C_{new}-D_{new}\\C_y^{new}&=A_{new}-B_{new}-C_{new}-D_{new}\\C_z^{new}&=A_{new}+B_{new}-C_{new}-D_{new}\end{aligned} \tag{13}$$

where

$$\begin{aligned}A_{new}&=F_{Ox_3},\quad B_{new}=\frac{1}{N_3}\left[(A+C)DB\right]\\C_{new}&=\frac{1}{2P_3}\left[A^2D+(B^2+C^2)A+D^2C\right]\\D_{new}&=\frac{1}{P_3}\left[AD^2+CB^2\right]\end{aligned} \tag{14}$$

and P_3 the probability of success

$$P_3=\frac{1}{2}\left[A^3+(3B^2+D^2)C+(3A+D)AD+2(A+C)BD+C^3\right] \tag{15}$$

Now assume that the pairs in the initial ensemble are not identical i.e with different $c_i, i=1,2,3$ and with different fidelities. Alice and Bob want to perform the Ox_3. To achieve this goal, they pick three pairs of the form

$$\rho=\frac{1}{4}(1+c_{xi}\sigma_x\tau_x-c_{yi}\sigma_y\tau_y+c_{zi}\sigma_z\tau_z),\quad i=1,2,3 \tag{16}$$

They perform all the required local operations as described above. After one iteration, they will get a new ensemble, with a new fidelity, to be used for the

arXiv:0804.1538v1 [quant-ph] 9 Apr 2008

More Efficient Purifying scheme via Controlled- Controlled NOT Gate

N. Metwally [1]and A.-S. Obada [2]

[1] *Math. Dept., Faculty of Science, South Valley University, Aswan, Egypt.*

[2] *Math. Dept., Faculty of Science, Al-Azhar University, Cairo, Egypt.*

Abstract

A new modified version of the Oxford purification protocol is proposed. This version is based on the controlled-controlled NOT gate instead of controlled NOT in the original one. Comparisons between the results of the new version and the original and an earlier modification are given. It is found that the new version converges faster and consumes fewer initial qubit pairs of low fidelity per final qubit pair of high fidelity.

1 Introduction

It is well known that to perform most of the quantum information schemes efficiently, one requires maximally entangled states to be performed. However in reality, it is mandatory to consider the effect of the decoherence. In this situation, the maximally entangled states turn into partially entangled or product states. Therefore, these schemes my not be realized faithfully. Thus purifying these states is of a great importance in the context of quantum information. The entanglement purification, that is often required, distills a small number of strongly entangled pairs of qubits from a large number of weakly entangled pairs. This can be achieved by using local quantum operations, classical communication and measurements. Bennett et. al have proposed the first entanglement purification scheme which is called the IBM protocol [1]. This protocol assumes that the initial states are of Werner type state. The initial density state for the IBM protocol is given by: $\rho = x|\psi^-\rangle\langle\psi^-| + \frac{1-x}{4}I$ which means that an x fraction of the singlet state $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ [2] and the rest is randomized . Another standard protocol has been proposed by Deutsch

[1] e. mail:Nasser_ Metwally@hotmail.com

et al. and it is called the Oxford protocol [3]. This protocol is designed for quantum cryptography. The initial density operator for this protocol takes the form: $\rho_{Ox} = A|\phi^+\rangle\langle\phi^+| + B|\psi^-\rangle\langle\psi^-| + C|\psi^+\rangle\langle\psi^+| + D|\phi^-\rangle\langle\phi^-|$ where $|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ are the Bell basis. Since then many theoretical [4] and experimental[5] schemes have been proposed.

The standard protocols [1,3] are based on the controlled NOT operations, CN and Bell state measurements. The IBM protocol has been improved by Feng et al [6], where they considered the controlled-controlled NOT operation (CCN) instead of CN. They showed that the new version is more efficient than the original one. Because in order to get a final state of certain fidelity from pairs of the same fidelity, the successful purification probability is larger and the amount of resources minimally consumed is less. Also the Oxford protocol has been improved by Metwally, where in his version the usual local unitary transformations are only performed when they are really helpful [7]. For some initial states this modification makes the new version converges faster, more efficient and needs fewer operations. For some other initial states the two versions are equivalent.

In this *contribution*, we study the Oxford protocol in the dynamical variables i.e., Pauli's operators, σ_i and τ_i, where $i = 0, x, y, z$ for the first and the second qubit respectively. In this current version we consider the CCN operation instead of the CN. We see that the modification makes the suggested version more efficient. In section 2,we describe briefly the Oxford protocol Ox_1 and its first modification Ox_2[7]. Also we achieve the CN operation using the dynamical variables. Section 3 is devoted to a study of the second modified version, Ox_3. A comparison of the three protocols is discussed in section 4. Finally we summarize our results in section 5.

2 The Oxford protocol, Ox_1 and the first modified version, Ox_2

Assume that Alice and Bob are given an ensemble of the so called generalized Werner states or self transposed states [8], or simply Bell-diagonal states [1]and they are asked to use the Oxford protocol to purify them. The users pick two pairs of the form

$$\rho^{(1)} = \frac{1}{4}(1 + c_x\sigma_x^{(1)}\tau_x^{(1)} - c_y\sigma_y^{(1)}\tau_y^{(1)} + c_z\sigma_z^{(1)}\tau_z^{(1)}) \tag{1}$$

where

$$1 \geq |c_x| \geq |c_y| \geq |c_z| \geq 0 \tag{2}$$

the order being a matter of convention. These coefficients $c_i, i = x, y, z$ are related to the coefficient of the original Oxford protocol by the following relations:

$$\begin{aligned} c_x &= A - B + C - D \\ c_y &= A - B - C - D \\ c_z &= A + B - C - D \end{aligned} \tag{3}$$

The initial fidelities of states (1) are given by:

$$F_1 = \mathrm{tr}\left\{\rho^{(1)}\rho^{(1)}_{\phi^+}\right\} = \frac{1}{4}(1 + c_x + c_y + c_z) \tag{4}$$

where

$$\rho^{(1)}_{\phi^=} = \frac{1}{4}(1 + \sigma_x^{(1)}\tau_x^{(1)} - \sigma_y^{(1)}\tau_y^{(1)} + \sigma_z^{(1)}\tau_z^{(1)}). \tag{5}$$

Assume that Alice and Bob want to purify their pairs by using the *first* modified Oxford protocol Ox_2. To achieve this aim, they perform the Bilateral CN operation, see table 1, on the pairs, followed by measuring the target qubit(second pair) in the computational basis. They measure the z components of the target spin $\sigma_z^{(2)}$ and $\tau_z^{(2)}$. They keep those first pairs for which they get the same results for the measurements and discard the others. After one step purification, they get

$$\rho_{Ox_2} = \frac{1}{4}\left[1 + \frac{c_x c_x' + c_y c_y'}{1 + c_z c_z'}\sigma_x\tau_x - \frac{c_x c_y' + c_y c_x'}{1 + c_z c_z'}\sigma_y\tau_y \frac{c_z + c_z'}{1 + c_z c_z'}\sigma_z\tau_z\right] \tag{6}$$

this is another new Bell state with fidelity,

$$F_{Ox_2} = \frac{1}{4P_1}\left[(1 + c_z)^2 + (c_x + c_y)^2\right] \tag{7}$$

	$I^{(2)}$	$\sigma_x^{(2)}$	$\sigma_y^{(2)}$	$\sigma_z^{(2)}$
$I^{(1)}$	1	$\sigma_x^{(1)}\sigma_x^{(2)}$	$\sigma_y^{(1)}\sigma_x^{(2)}$	$\sigma_z^{(1)}$
$\sigma_x^{(1)}$	$\sigma_x^{(2)}$	$\sigma_x^{(1)}$	$\sigma_y^{(1)}$	$\sigma_z^{(1)}\sigma_x^{(2)}$
$\sigma_y^{(1)}$	$\sigma_z^{(1)}\sigma_y^{(2)}$	$\sigma_y^{(1)}\sigma_z^{(2)}$	- $\sigma_x^{(1)}\sigma_z^{(2)}$	$\sigma_y^{(2)}$
$\sigma_z^{(1)}$	$\sigma_z^{(1)}\sigma_z^{(2)}$	$-\sigma_y^{(1)}\sigma_y^{(2)}$	$\sigma_x^{(1)}\sigma_y^{(2)}$	$\sigma_z^{(2)}$

Table 1
Bilateral CN operation between the two qubits which is defined by $\sigma_\mu^{(1)}$ and $\sigma_\mu^{(2)}$. The same table is applied to the two qubits $\tau_\mu^{(1)}$ and $\tau_\mu^{(2)}$.

where $P_1 = \frac{1}{2}(1 + c_z^2)$, is the probability that Alice and Bob obtain coinciding outcomes in the measurement of target pair[7]. Now Alice and Bob have a new ensemble described by (6). If this ensemble does not obey the ordering required by (2), then Alice and Bob use local rotations to bring the state into the wanted form. These are rotations by $\pi/2$ about the x, y or z axis, namely

$$U_{12j} = e^{i\pi(\sigma_j - \tau_j)} \quad \text{and} \quad j = x, y, z. \tag{8}$$

In fact it is only necessary to ensure that $|c_z|$ is smaller than $|c_x|$ and $|c_y|$; the relative size of $|c_x|$ and $|c_y|$ does not matter. In the standard protocol, Ox_1 [1], Alice and Bob perform the transformation (8) in $x-$ direction on all pairs. This operation changes the positions of c_y and c_z. After applying the Bilateral CN operation and measuring the target qubits, Alice and Bob get a new ensemble with fidelity

$$F_{Ox_1} = \frac{1}{4P_2}\left[(1 + c_y)^2 + (c_x + c_z)^2\right] \tag{9}$$

where $P_2 = \frac{1}{2}(1 + c_y^2)$ is the probability that Alice and Bob's measurements are the same.

3 The second modified protocol, Ox_3

Before performing this protocol, one needs to describe the controlled-controlled Not, CCN. It is a three qubit gate, two of them are used as a control qubit and the third is a target. Mathematically it takes the following form,

$$\begin{aligned} CCN = \frac{1}{4}\Big[&(1 + \sigma_z^{(1)})(1 + \sigma_z^{(2)})\sigma_x^{(3)} + (1 + \sigma_z^{(1)})(1 - \sigma_z^{(2)}) \\ &+ (1 - \sigma_z^{(1)})(1 + \sigma_z^{(2)}) + (1 - \sigma_z^{(1)})(1 - \sigma_z^{(2)})\Big] \end{aligned} \tag{10}$$

The target qubit pairs change only when the two control qubits are in the state 1. In a generic form one can write its effect as $CCN|abc\rangle = |ab, c \oplus a.b\rangle$. As an example it transforms the vector $|\phi_1^+\phi_2^+\phi_3^-\rangle$ to $\frac{1}{2}[|\phi_1^+\phi_2^+\phi_3^-\rangle + |\phi_1^-\phi_2^+\phi_3^-\rangle + |\phi_1^+\phi_2^-\phi_3^-\rangle - |\phi_1^-\phi_2^-\phi_3^-\rangle]$. It is possible to consider the effect on the dynamical variables, but its form is too complicated to be written in this text.

Assume that Alice and Bob are given an ensemble of identical pairs in the form of equation (1). To perform the second modified version of the Oxford protocol Ox_3, they pick three pairs and both of them perform the transformation (8) on all pairs. After applying the CCN operations , they measure the target qubits

in the projection $|\phi^+\rangle_{A_1A_2}\langle\phi^+|\otimes|\phi^+\rangle_{B_1B_2}\langle\phi^+|+|\phi^-\rangle_{A_1A_2}\langle\phi^-|\otimes|\phi^-\rangle_{B_1B_2}\langle\phi^-|$, where A_1A_2 and B_1B_2 stands for the first and the second qubits for Alice and Bob respectively. They will keep those pairs for which the measurement results coincide. These pairs are used for the second round. After one step purification they get a new ensemble of states,

$$\rho_{Ox_3} = \frac{1}{4}(1 + c_x^{new}\sigma_x\tau_x + c_y^{new}\sigma_y\tau_y + c_z^{new}\sigma_z\tau_z) \tag{11}$$

with a fidelity

$$F_{Ox_3} = \frac{1}{2P_3}\Big[(A^2 + D^2)A + (B^2 + C^2)C\Big] \tag{12}$$

and,

$$\begin{aligned} C_x^{new} &= A_{new} - B_{new} + C_{new} - D_{new} \\ C_y^{new} &= A_{new} - B_{new} - C_{new} - D_{new} \\ C_z^{new} &= A_{new} + B_{new} - C_{new} - D_{new} \end{aligned} \tag{13}$$

where

$$\begin{aligned} A_{new} &= F_{Ox_3}, \quad B_{new} = \frac{1}{N_3}\left[(A + C)DB\right] \\ C_{new} &= \frac{1}{2P_3}\Big[A^2D + (B^2 + C^2)A + D^2C\Big] \\ D_{new} &= \frac{1}{P_3}\Big[AD^2 + CB^2\Big] \end{aligned} \tag{14}$$

and P_3 the probability of success

$$P_3 = \frac{1}{2}\Big[A^3 + (3B^2 + D^2)C + (3A + D)AD + 2(A + C)BD + C^3\Big] \tag{15}$$

Now assume that the pairs in the initial ensemble are not identical i.e with different $c_i, i = 1, 2, 3$ and with different fidelities. Alice and Bob want to perform the Ox_3. To achieve this goal, they pick three pairs of the form

$$\rho = \frac{1}{4}(1 + c_{xi}\sigma_x\tau_x - c_{yi}\sigma_y\tau_y + c_{zi}\sigma_z\tau_z), \quad i = 1, 2, 3 \tag{16}$$

They perform all the required local operations as described above. After one iteration, they will get a new ensemble, with a new fidelity, to be used for the

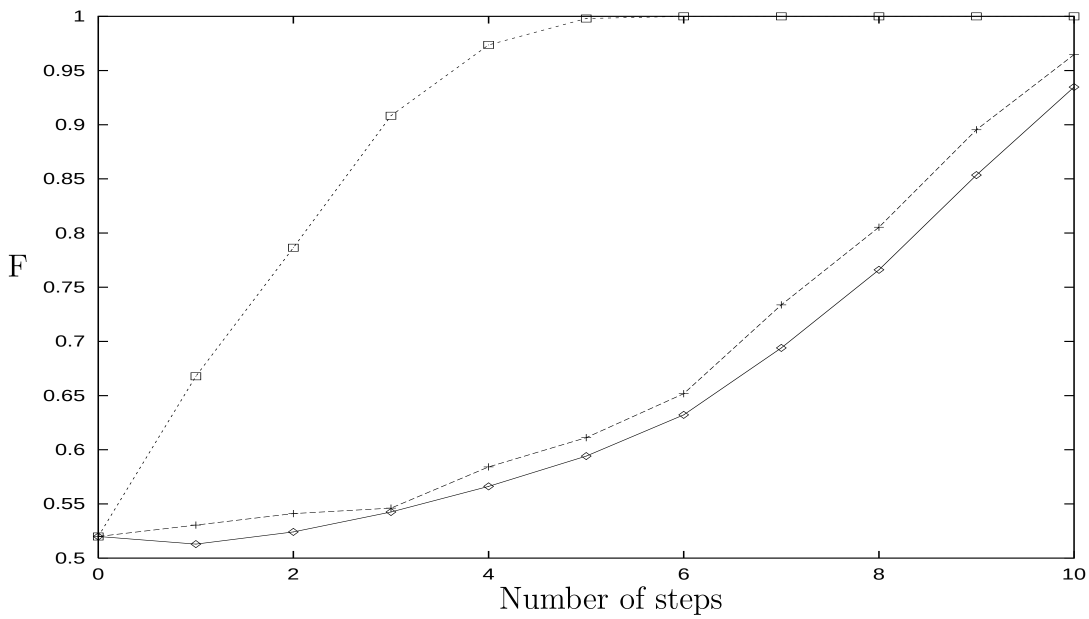

Fig. 1. The Fidelity of the purified pairs, the dot line represents the Ox_3, the dashed line for Ox_2 and the solid line for the original protocol Ox_1. The initial fidelity of the pairs, $F = 0.52$.

second round. In this case the fidelity is given by

$$F = \frac{1}{2P_d}\left[(A_1A_2 + D_1D_2)A_3 + (B_1B_2 + C_1C_2)C_3\right] \tag{17}$$

where P_d is the probability of success,

$$\begin{aligned} P_d = \frac{1}{2}\Big[& A_1A_2(A_3 + D_3) + (B_1B_2 + C_1C_2 + D_1D_2)(A_3 + C_3) \\ & + 2(A_1D_2 + D_1A_2 + B_1C_2 + C_1B_2)(B_3 + D_3)\Big] \end{aligned} \tag{18}$$

4 Discussion

To study the efficiency of the protocols: the original one Ox_1, the first modified one, Ox_2 and the second modified one Ox_3, we consider an ensemble of identical states given by (1). Lat us assume that this ensemble has an initially fidelity, $F = 0.52$. In Fig.(1), we plot the fidelity of the surviving states after each step as a function of the number of iteration. As a first remark, the fidelity of the purified state using the Ox_2 and Ox_3 after one step is larger than that obtained using the standard protocol Ox_1. It decreases for the Ox_1 and then increases, but for the modified ones it always increases. Concerning the fidelity

after one step obtained by using Ox_3 it is much larger that obtained from Ox_2. Since the fidelity in each next step depends on the previous one, the final state in the modified protocols converges faster than in the standard one. Also for the Ox_3 it converges much faster than Ox_2. The number of steps needed in the modified protocols are fewer than those in the standard one. In table (2) there is a comparison of the three protocols. It is clear that, in order to get a state with a fidelity $\simeq 0.8$, one needs 9 steps for the Ox_1 and 8 steps for the Ox_2 and 3 steps for the Ox_3. The probability of success in each step, for the original protocol is larger than the modified ones. To complete comparing

protocol	Fidelity	number of iterations	consumed pairs
Ox_1	0.853	9	256
Ox_2	0.805	8	128
Ox_3	0.843	3	9

Table 2
Comparison between the Ox_1 and its modified versions Ox_2 and Ox_3.

the efficiency between the three protocols, we have to examine the consumed pairs in each protocol. We know that the users in each step needs two pairs for the Ox_1 and Ox_2 protocol while three pairs for the Ox_3 are needed. In each success step, they consume one pair for the Ox_1 and Ox_2 but two pairs for the Ox_3. Table (2) shows the number of the consumed pairs in each protocol to get a certain fidelity. From this table it is clear that the resource consumed in the modified versions are fewer than the original one.

5 Summary

The new proposed version Ox_3 is more efficient than Ox_1 and Ox_2 for the following reasons:(i) The final state converges faster than the two other protocols. (ii) The steps needed to get a state with a certain fidelity are fewer than those needed if the other protocols are used. (iii)The consumed sources are much fewer. (iv) The new version, Ox_3 is efficient for any set of initial states, while the Ox_2 and Ox_1 are the same for the set of Werner states. However, we would point out to the only disadvantage of this protocol namely: the successful purification probability is smaller than the original one, however the Ox_3 is much better than Ox_2.

Acknowledgments

We thank the referees for their objective comments that improved the text on many points.

References

[1] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin and W. K. Wottor, Phys. Rev. Lett.**76**,722 (1996); C. Bennett, D. P. DiVincenzo, J. A. Smolin and W. K. Wootter, Phys. Rev. A **54**, 3824 (1996).

[2] R. F. Werner, Phys. Rev. A **40**, 4277 (1989); A. Peres, Phys. Rev. Lett.**77**, 1413 (1996).

[3] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. popescu and A. Sanpera, Phys. Rev. Lett **77**,2818(1996); C. Macchiavello, Phys. Lett. **A246**, 385 (1998).

[4] J. -W. Pan et al., Phys. Rev. Lett. **80**, 3819 (1998);Bao-Sen Shi, Yun-Kun-Jiang and Guang-Ca Guo Phys. Rev. A **62**, 054301 (200); J. -W. Pan, C. Simon, C. Brakner and A. Zeiliner, Nature**410**(2002); Liu Ye, Chun-Mei Yao and Guang- Can Gu, J. Opt. B **3**, 21 (2002) and W. Dur and H.-J. Briegel Phys. Rev. Lett. **90**, 067901 (2003).

[5] J. W. Pan, S. Gasparoni, R. Ursin, G. Weihs and Zilinger, Nature **423**, 417 (2003).

[6] Xun-Li Feng, Shang-Qing Gand Zhi-Zhan Xu,Phys. Lett. **A271**, 44 (2000).

[7] N. Metwally, Phys. Rev. A **66**, 054302 (2002).

[8] B.-G. Englert and N. Metwally J. Mod. Opt. **47**, 221 (2000); B.-G. Englert and N. Metwally, *Mathematics of Quantum computation*, edit by R. Brylinski and G. Chen (CCR, Boca Raton, FL, 2002), pp. 25-75.